REMARKS

Applicant thanks the Examiner for the opportunity of a telephone interview conducted on July 14, 2005. During the interview, Applicant's undersigned representative cited independent claim 131, which requires inserting received data comprising a public key for a digital signature into a predetermined bits portion of the digital data, and explained that the cited references do not disclose or suggest such features. The Examiner agreed that the claims probably distinguish over the cited references, and proposed clarifying claim amendments to clarify features recited. The foregoing will serve as Applicant's Statement of the Substance of the Interview.

Claims 130-133 are the claims currently pending in the Application.

Claims 130-133 are amended to clarify features recited thereby. However, Applicant does not agree with the necessity of making the proposed claim amendments, as the claim amendments are not believed to be necessitated by the prior art, and are not believed to be required by applicable law or regulation. The claim amendments are made to expedite prosecution of the Application.

Rejection of Claims 130-133 under 35 U.S.C. § 103

Claims 130-133 are rejected under 35 U.S.C. § 103 as being obvious from Muratani et al., U.S. Patent No. 6,061,451 in view of Ruppert et al., U.S. Patent No. 5,640,002. This rejection is traversed.

One of the problems recognized and solved by Applicant's claimed invention is that a digital signature for authenticating digital data, such as for example a digital image, be transmitted as part of the same data set as the digital data.[1] For example, according to an aspect of Applicant's claimed invention, a digital signature is inserted into a portion of the digital data determined previously, and this digital signature is then used to authenticate the digital data.

For at least the following reasons, Applicant's claimed invention is neither anticipated by nor obvious from the cited references. By way of example, independent claims 130-133 require inserting received data comprising a digital signature including a public key into a predetermined bits portion of the digital data.

Muratani discloses decrypting data that is received in an encrypted form from a network (Muratani, Abstract); for example, encrypted data received via a settop unit is descrambled by a descramble circuit of a security module that is connected to the settop unit (Muratani, Abstract; Fig. 2).

The Examiner acknowledges that Muratani does not disclose or suggest a digital signature inserted into the digital data, nor inserting a public key for the digital signature into a predetermined bits portion of the digital data (or into the digital image, per claim 133), as inter alia, required by independent claims 130-133. However, the Examiner alleges that Ruppert discloses these features.

Ruppert discloses a portable radio frequency bar code ID tag reader of the type used for example, at a supermarket checkout to authenticate articles by accessing a factory computer using the serial number of the article scanned from a radio frequency ID tag on the article. (Ruppert, Abstract.) Ruppert discloses that a

[1] The present discussion illustrates aspects of Applicant's claimed invention. Applicant does not represent that every embodiment of Applicant's claimed invention necessarily embodies or performs the solutions herein discussed or addresses the problems herein identified.

computer sends its public key to a factory host computer (Ruppert, Figure 41, Reference Numeral 749); and that the factory computer uses its secret key to authenticate a serial number list, generates an authentication message, generates authentication signature of the message, and encrypts the authentication signature and authentication signature message using the public key (Ruppert, Figure 41, Reference Numerals 753-759).

Ruppert does not disclose or suggest inserting the received data comprising a public key for a digital signature into a predetermined bits portion of the digital data, as inter alia required by independent claims 130-132. First, Ruppert does not disclose or suggest a predetermined bits portion of digital data into which received data are inserted. That is, Ruppert does not disclose or suggest digital data comprising a predetermined bits portion into which some other data for authentication are inserted.

Second, since Ruppert does not disclose or suggest this feature, Ruppert is incapable of disclosing or suggesting inserting received data comprising a public key for a digital signature into the predetermined its portion of the digital data, as further required by independent claims 130-132. Moreover, Ruppert does not disclose or suggest inserting the received data comprising a public key for a digital signature into a predetermined bits portion of the digital image, as inter alia required by independent claim 133. Therefore, this rejection should now be withdrawn.

For at least the reasons set forth in the foregoing discussion, Applicant believes that the Application is now allowable and respectfully requests that the Examiner reconsider the rejections and allow the Application. Should the

Examiner have any questions regarding this Amendment, or regarding the Application generally, the Examiner is invited to telephone the undersigned attorney.

Respectfully submitted,

George Brieger
Registration No. 52,652

SCULLY, SCOTT, MURPHY & PRESSER
400 Garden City Plaza
Suite 300
Garden City, New York 11530
(516) 742-4343, Ext. 503

GB:ar